Network and Information Security Management Discussion Forum 2

*1 - **Learning Outcomes***

- *Gather and synthesise information from multiple sources (including Internet security alerts and warning sites) to aid in the systematic analysis of security breaches and issues*

Discussion topic

This discussion is based on our basic scans of a vulnerable website.

- You should demonstrate that you understand the topic covered and ensure you use references to academic literature (journals, books, reports, etc.).

My Initial post

Our group decided to scan the website individually and then share the results in our group. This exercise tasked us to use a variety of tools to scan a vulnerable website using tools that are readily available or easily installed on Windows and Linux.

For this task, I used a virtualisation of Kali Linux on a Windows 11 laptop as well as the Windows Command utility for webpage https://customersrus.co.uk.

As this was the first time to use Kali Linux and its tools, I was not confident about the accuracy or reliability of the processes and my results. The first utility I used was >*Host customersrus.co.uk,* and it returned the IP address 68.66.247.187. which allows the *host* command to discover the IP address for the specific domain under the DNS (sethusubramanian, 2018).

Next, I used a Nmap, mtr, traceroute and tracert to get discover how many hops to the website, and to see how if there was consistency. The first scan involved traceroute returning two hops in 308ms. Nmap traceroute -sn Pn –tr returned three hops 1.83ms using TCP/port 80. Interestingly, it picked up my VPN server in Singapore.

Windows' tracert took 18 hops and 505ms, and Nmap --tr -f -pn took 16 hops and 305ms to discover the website. According to (Buzdar, 2022) the Linux mtr is simpler version of traceroute and allows to specify TCP SYN instead of using ICMP Echo requests. I used mtr -r –tcp, and it took 2 hops and 373.8ms to find the domain.

Dig and nslookup scan results showed only one IP address, Whois showed the registered contact as enom.com with four servers at .a2 hosting.com. I used the website search tool called MX toolbox to find the MX records as my Linux Kali command line search was unsuccessful. The result came back as mail.cusomtersrus.co.uk with the IP address. Admin (2020) states the Dig command with MX option is great tool for querying DNS and domain MX records. Finally, the current location of the static IP address was in Ann Arbor, Michigan, USA according to WhatIsMyIPAddress.com (2022).

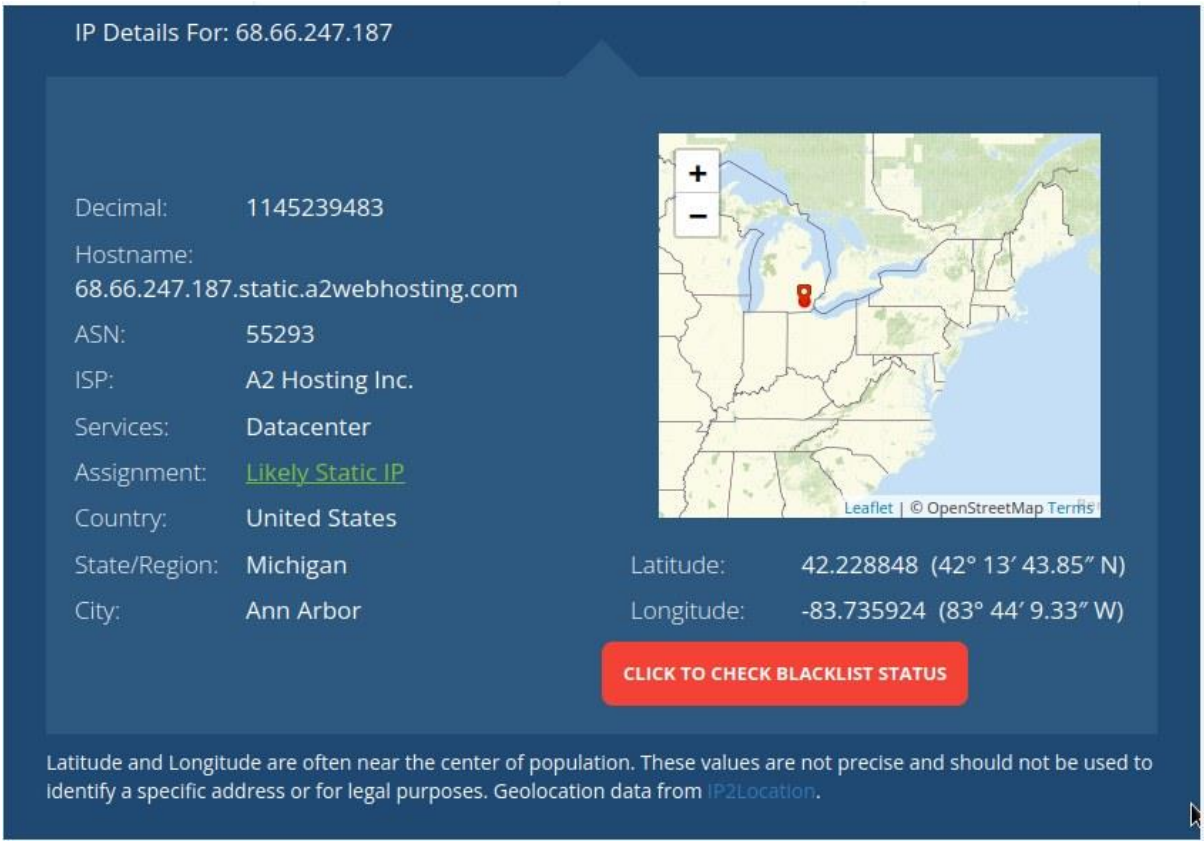
References

Admin (2020) How to check domain's MX (mail exchange) records using dig command on Linux. [online] Linux Tutorials - Learn Linux Configuration. Available from: https://linuxconfig.org/how-to-check-domain-s-mx-mail-exchange-records-using-dig-command-on-linux [Accessed 24 Mar. 2022].

Buzdar, K. (2022) How to use the Linux mtr (My Traceroute) command – VITUX. vitux.com. Available from: https://vitux.com/how-to-use-the-linux-mtr-command/#:~:text=1%20How%20to%20use%20the%20Linux%20mtr%20%28My [Accessed 24 Mar. 2022].

Sethusubramanian (2018) host command in Linux with examples. GeeksforGeeks. Available from: https://www.geeksforgeeks.org/host-command-in-linux-with-examples/?msclkid=5bb067f7af6911ec89456254fc70837d [Accessed 29 Mar. 2022].

WhatIsMyIPAddress.com. (2022) What Is My IP Address? IP Address Tools and More. Available from: https://whatismyipaddress.com/ [Accessed 24 Mar. 2022].



2 - The current location of the static IP address was in Ann Arbor, Michigan, USA according to WhatIsMyIPAddress.com (2022).

Response from Beran:

Hi Jonathan,

Thank you for initiating this discussion.

As you mentioned tracert scanning resulted in different variations. Can you also research and try Paris traceroute to compare your results with that of classic traceroute.

Regards, Beran

My response to Beran:

Thanks Beran,

This time I used >tracert -d customersrus.co.uk

Using tracert -d prevented the hostname being resolved which resulted in only the IP address being scanned. There are now 15 hops and much quicker time than just a basic tracert scan. However, the initial hope and time is due to connecting to the VPN server in UK. For comparison, using tracert -d on Google.co.uk returned 10 hops but still the time is long.

I am having issues installing paris-traceroute on Linux for some reason. I will update if I can get it to work in the future.

Facebook, Twitter, and LinkedIn (2021) *How to Use the Tracert Command in Windows*. Lifewire. Available from: https://www.lifewire.com/tracert-command-2618101

Peer response to Andrijana:

Hi Andijana,

I had similar high ping times and multiple hops. Though I use a VPN service, and I frequently have to change servers due to its responsiveness and my needs. According to Crawford (2019), using a VPN service does impact ping as it has routed through a server and coupled with encryption and decryption processes as well as other users which can cause latency. Other ways to mitigate latency when using VPN service is to choose a server closest to one's physical location, use a reputable VPN provider, and chose a suitable protocol suited for one's needs. That is, if you want to sacrifice privacy for speed in the case of gaming; for example, PPTP versus OpenVPN protocols.

Crawford, D. (2019) How to test ping on a VPN | Step by step guide (With images). ProPrivacy.com. Available from: https://proprivacy.com/vpn/guides/vpn-ping?msclkid=47923191b95611ec98184ff470ab8ddf [Accessed 11 Apr. 2022].

Peer response too Agne and Kevin:

Hi Agnes and Kevin,

It was interesting to read your posts about web-based IP addresses. This made me curious about my initial findings as I too stated Ann Arbor was the physical location. I returned to my scans and did some digging.

I now used Shodan (2022) and searched 66.66.24.187; it returned Amsterdam, Netherlands. It also showed which ports are open and what services are being used. Port 21 states that Pureftpd.org (FTP Unix server) is using it with an SSL certificate:

Subject: C=US, ST=Michigan, L=Ann Arbor, O=A2 Hosting, Inc., CN=*.a2hosting.com

The information also showed that the SSL certificate was issued by digicert, a digital security company. Using the digicert's SSL Certificate Checker, I inputted the server address 'a2hosting.com', and it returned this information:

DNS resolves a2hosting.com to 104.18.132.225

HTTP Server Header: cloudflare

TLS Certificate

Common Name = www.a2hosting.com

Organization = A2 Hosting, Inc.

City/Locality = Ann Arbor

State/Province = Michigan

Country = US

Subject Alternative Names = www.a2hosting.com, a2hosting.com

Using Shodan again, I searched 104.18.132.225 which returned the following:

General Information

Hostnames

a2hosting.com, www.a2hosting.com

Domains

A2HOSTING.COM

Country

United States

City

San Francisco

Organization

Cloudflare, Inc.

ISP

Cloudflare, Inc.

ASN

AS13335

Using Shodan again, I searched A2hosting.com domain records, and it listed hundreds of domains and IP addresses.

CloudFlare (2022) is a Content Delivery Network (CDN), networking, firewall provider which helps entities to cache files in edge locations globally. Interestingly, I used their Cloud flare system status page, and they have an operational data centre in Amsterdam. This makes sense to have cache files near the website/server.

Next, I searched 'A2hosting.com Ann Arbor' and found their PO Box address, website, telephone, Facebook, and LinkedIn information. Amazingly, A2hosting is named after Ann Arbor (Ax2) and has existed since 2001. I used their 'hosting is it right for you' tool to see if I could mimic 'customersrus.co.uk' business 'needs'. I selected:

- New to web hosting
- a few hundred visitors a week
- business website
- small budget

it returned 'Shared Web Hosting' which is a shared server. Also, a2.hosting offer add-ons such SSL certificates including digicert and Cloudflare CDN. It is worth noting that a2hosting has a data centre in Amsterdam.

I rechecked my previous scans and noticed my tracert scan showed this:

- v402.R2.NL1.a2webhosting [209.124.94.239]
- 66.66.247.187 static.a2webhosting.com [68.66.247.178]

Using Ipinfo (2022), it listed 209.124.94.239 in Amsterdam. In other words, the packets' last two hops were sent to Amsterdam and finishing in Ann Arbor.

Finally, a.2hosting (2022) offer further information on their Knowledge Base 'Off-shore IP addresses' section. They state there is no real way to know for certain an IP address location unless a warrant is issued, and that due to a finite number of IP address, if a.2hosting leases IP addresses from a US provider then it will have a US geolocation even if the server is in foreign country.

It seems that the hosting company is headquartered in Ann Arbor, USA but has data centres in many countries including Netherlands, and it offers CDN and SSL third party services. The web site 'customersrus.co.uk' is using a.2hosting shared server located in Amsterdam, and as it is using a US leased IP address from a.2hosting, the final destination shows a US location.

Reference list

Cloudflare. (2022) Cloudflare CDN | Content Delivery Network. Available from: https://www.cloudflare.com/cdn/.

Ipinfo.io. (2013) IP Address API and Data Solutions - geolocation, company, carrier info, type and more - IPinfo IP Address Geolocation API. Available from: https://ipinfo.io/.

Shodan (2013). Shodan. Available from: https://www.shodan.io/.

www.a2hosting.com. (2022a) Using Cloudflare. Available from: https://www.a2hosting.com/kb/add-on-services/cloudflare [Accessed 14 Apr. 2022].

www.a2hosting.com. (2022b) Web Hosting Services | 2020's BEST Shared Hosting. Available from: https://www.a2hosting.com/web-hosting.

www.digicert.com. (2022) SSL Certificate Checker - Diagnostic Tool | DigiCert.com. Available from: https://www.digicert.com/help/ [Accessed 14 Apr. 2022].

My summary

This exercise tasked us to use a variety of tools to scan a vulnerable website using tools that are readily available or easily installed on Windows and Linux. I enjoyed the practical aspect and reading other posts; I then questioned my findings and looked deeper for the answer: where is the location of the website?

My initial findings showed that my scans had many hops and high latency. This could be attributed to my location as I am based in China, and I need to use VPN service. Using the 'host' utility, I scanned 'customersrus.co.uk' which gave me IP address 68.66.247.187 which I then used a web-based to geolocate the website. The result showed Ann Arbor, USA.

Spurred on by Angelides and Peuhkurinen's (2022) responses, I further investigated the geolocation of 'customersrus.co.uk'. I used Shodan to analysis the IP address and related records, and after following the digital trail, my conclusion is Ann Arbor is the headquarters of a2hosting with a data centre in Amsterdam, Netherlands. As a.2hosting has a limited number of IP addresses and a US company, the leased IP address originates from USA whereas the website's server is in Amsterdam.

The techniques used, exploring the digital records, and reading other classmates' posts really helped me to become a better cyber security student.

References

Angelides, A. (2022) Group 1 - initial post Available from: https://www.my-course.co.uk/mod/hsuforum/discuss.php?d=303719#/mod/hsuforum/discuss.php ?d=303719&postid=1057876 [Accessed 15 Apr. 2022].